Fast Integral Bases Computation

Adrien Poteaux, Martin Weimann

Fast Integral Bases Computation

Adrien Poteaux[1] and Martin Weimann[2]

[1] Univ. Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL, F-59000 Lille, France
adrien.poteaux@univ-lille.fr
https://www.fil.univ-lille.fr/~poteaux/
[2] LMNO, Université de Caen-Normandie
martin.weimann@unicaen.fr
https://weimann.users.lmno.cnrs.fr/

Abstract. We obtain new complexity bounds for computing a triangular integral basis of a number field or a function field. We reach for function fields a softly linear cost with respect to the size of the output when the residual characteristic is zero or big enough. Analogous results are obtained for integral basis of fractional ideals, key ingredients towards fast computation of Riemann-Roch spaces. The proof is based on the recent fast OM algorithm of the authors and on the `MaxMin`algorithm of Stainsby, together with optimal truncation bounds and a precise complexity analysis.

Keywords: Fields, Fractional ideals, Integral bases, OM algorithm.

1 Introduction

Let A be a principal ideal domain with field of fractions K and let L/K be a separable field extension of degree d. Denote B the integral closure of A in L. It is a free A-module of rank d and an integral basis of L/K is a collection $b_1, \dots, b_d \in B$ that form a A-basis of B.

This paper intends to give new complexity bounds for computing an integral basis and, more generally, for computing an A-basis of an arbitrary fractional ideal of L. These fundamental problems of computer algebra are cornerstones towards more advanced computational issues both in algebraic number theory and in algebraic geometry, such as developing a fast arithmetic of ideals in number fields [7] or computing Riemann-Roch spaces in function fields [2,14].

In all of the sequel, we will assume that $L = K(\theta)$ is generated by the root θ of a degree d monic separable irreducible polynomial $f \in A[x]$. Under this assumption, there exists an integral basis of L/K of shape

$$\mathcal{B} = \left(1, \frac{g_1(\theta)}{a_1}, \dots, \frac{g_{d-1}(\theta)}{a_{d-1}}\right) \tag{1}$$

where $g_i \in A[x]$ is monic of degree i, $a_i \in A \setminus \{0\}$ and $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_{d-1}$. We call such a basis a *triangular integral basis*. This specific shape has various algorithmic advantages, in particular for computing Hermite normal forms or Popov forms.

Model of computation. For the sake of simplicity, we will express our complexity results in the case $A = k[t]$ (resp. $A = \mathbb{Z}$). We work with computation trees [6, Section 4.4]. When considering $A = k[t]$, we use an algebraic RAM model, counting only the number of arithmetic operations in k. For $A = \mathbb{Z}$, we consider the Boolean RAM model.

We classically denote $\mathcal{O}()$ and $\tilde{\mathcal{O}}()$ to respectively hide constant and logarithmic factors in our complexity results ; see e.g. [9, Chapter 25, Section 7]. We additionally let $\mathcal{O}_\epsilon(d) = \mathcal{O}(d^{1+\epsilon(d)})$ with $\epsilon(d) \to 0$. We have $\tilde{\mathcal{O}}(d) \subset \mathcal{O}_\epsilon(d)$, and freely speak of *almost linear* in d for both notations. As in [24], we express our complexity with $\mathcal{O}_\epsilon()$ because we deal with dynamic evaluation via the deterministic algorithm of [16]. Our results could be express with the $\tilde{\mathcal{O}}()$ notation using some Las Vegas sub-algorithm instead.

Discriminant and index. Our results will be expressed using the size functions $h(a) = \deg(a)$ when $A = k[t]$ (resp. $h(a) = \log(|a|)$ when $A = \mathbb{Z}$). Note that $h(a) = \sum_p v_p(a)h(p)$ where the sum runs over the primes p of A and v_p stands for the p-adic valuation. Let us denote $\Delta = \Delta_f$ the discriminant of f and $\Delta_{L/K}$ the discriminant of L/K. Both quantities are related by the formula

$$\Delta = D^2\,\Delta_{L/K} \tag{2}$$

where $D = D_f \in A$ is the index of f, generator of the index ideal $[B : A[\theta]]$. We denote for short $h_\Delta := h(\Delta)$, $h_D := h(D)$ and $h_{red} := \sum_{p^2|\Delta} h(p)$. Looking at the triangular basis (1), we observe that $D = ua_1 \cdots a_{d-1}$ for some unit $u \in A^\times$ and, up to reduce g_i modulo a_i, the basis $\mathcal{B}$ has global size $\mathcal{O}(dh_D)$, this bound being sharp. This observation suggests to emphasise the dependency of the complexity on the index D instead of the discriminant Δ which is classically considered in the literature (see e.g. [1,3,25]).

Global integral basis computation. Our main result is:

Theorem 1. *Suppose given a squarefree factorisation of the index D. There exists a deterministic algorithm which computes a triangular integral basis of L/K in less than*

1. *$\mathcal{O}_\epsilon(dh_D)$ operations in k if $A = k[t]$ with $char(k) = 0$ or $char(k) > d$,*
2. *$\mathcal{O}_\epsilon(d\,h_D + h_D^2)$ operations in k if $A = k[t]$ with $char(k) \leq d$,*
3. *$\mathcal{O}_\epsilon(d\,h_D + h_D^2)$ word operations if $A = \mathbb{Z}$.*

If we are only given the squarefree factorisation of the discriminant Δ, then a similar result holds, adding a cost $\mathcal{O}(d\,h_{red})$ to the complexity estimates.

We thus get a softly linear cost in case 1. In the other cases, the over-cost in h_D^2 is only due to the complexity of the OM algorithm [24] over small residual characteristic, so that *the result would become softly linear for all cases if we are able to improve the complexity of the OM algorithm.* In the last statement, the extra cost $\mathcal{O}(d\,h_{red})$ is needed to detect which prime divisors of Δ are prime divisors of D.

In the case $A = k[t]$, we have access to polynomial time squarefree factorisation, leading to the following total cost estimate:

Corollary 1. *Suppose $A = k[t]$. There exists a deterministic algorithm which computes a triangular integral basis of L/K in less than*

1. *$\mathcal{O}_\epsilon(d\, h_\Delta)$ operations in k if $char(k) = 0$ or $char(k) > d$,*
2. *$\mathcal{O}_\epsilon(d\, h_\Delta + h_D^2)$ operations in k otherwise.*

The algorithm returns as a byproduct the index D and the discriminant $\Delta_{L/K}$.

These results improve significantly [25, Theorem 3.5] which after Chinese remainder gluing leads to a global cost $\mathcal{O}_\epsilon(d^2\, h_\Delta + d\, h_\Delta^2)$. Up to our knowledge, this is the best complexity estimate in the literature. Note also [1] which leads to $\mathcal{O}_\epsilon(d^2\, h_\Delta)$ in the particular case $A = k[t]$ and $\mathrm{char}(k) = 0$, based on fast computation of Puiseux series (although the resulting integral basis is not triangular).

The complexity indicators h_D and h_{red} in Theorem 1 satisfy $h_D + h_{red} \leq h_\Delta$, and the difference may be significant, especially when wild ramification occurs.

Example 1. Consider $f = x^q + t^n x + t \in \mathbb{F}_q[t][x]$ with q a prime. We have $\Delta = t^{nq}$ while $D = 1$. We get $h_\Delta = qn$, $h_D = 0$, and $h_{red} = 1$. An integral basis is trivially $(1, \theta, \ldots, \theta^{d-1})$. Accordingly, Theorem 1 estimates the true cost $\mathcal{O}(d)$ to compute such a basis, while using h_Δ as a complexity indicator would lead to the bad estimate $\mathcal{O}_\epsilon(d^2 n)$, the integer n being arbitrarily large. See [11, Section 6] for further examples comparing $h_D + h_{red}$ and h_Δ in the case $A = \mathbb{Z}$.

Let us emphasise that Corollary 1 simply adds to Theorem 1 an extra cost $\mathcal{O}(d h_\Delta)$ due to the computation of Δ, plus $\tilde{\mathcal{O}}(h_\Delta)$ for its squarefree factorisation. Hence any progress for computing the discriminant would improve the complexity estimate of Corollary 1. There have been recent results in that direction in the case $k = \mathbb{F}_q$: it follows from [27] that there is a randomised algorithm of Monte Carlo type which computes the radical of Δ (and this is enough for our purpose) in softly optimal time in h_Δ.

Integral basis over a prime p. If we only want a p-integral basis at a given prime $p \in A$ (that is an A_p-basis of $B \otimes A_p$ over the localisation of A at p), we get similar complexity estimates than in Theorem 1, replacing h_D and h_{red} by their respective local contributions $v_p(D)h(p)$ and $h(p)$. There's no need to compute and factorise the discriminant in such a case. This result has to be compared to [25, Theorem 3.5] (triangular basis) or [3, Lemma 3.10] (non triangular basis).

The case of fractional ideals. In Section 4, we provide similar complexity results to compute integral basis of an arbitrary fractional ideal $I \subset L$, expressed now in terms of the size of the index $[I^* : A[\theta]]$ of the smallest multiple $I^* = \alpha I$, $\alpha \in K$ such that $B \subset I^*$, see Theorem 7. This is an important issue towards the computation of Riemann-Roch spaces in function fields.

Previous results. Classical methods for computing integral bases are variants of the Round-2 and Round-4 routines by Zassenhaus and Ford [8,13,15,23]. The central idea is to start from a known order $A[\alpha] \subset B$, and to enlarge it for each prime $p \in A$ dividing the discriminant of $A[\alpha]$ until we reach the maximal order B. Another strategy of local-to-global type was developed by Okutsu [20]: assuming given the local $\mathfrak{p}$-integral basis $\mathcal{B}_\mathfrak{p}$ for each prime ideals $\mathfrak{p} \subset B$ dividing a prime $p \in A$, one can compute multipliers $z_\mathfrak{p} \in L$ such that $\mathcal{B}_p = \cup z_\mathfrak{p}\mathcal{B}_\mathfrak{p}$ is a p-integral basis. Then, after reducing $\mathcal{B}_p$ to a triangular form, one can glue the various bases $\mathcal{B}_p$ into a global integral basis $\mathcal{B}$ by means of Chinese remainders. Later on, Montes [22] extended the ideas of Ore and MacLane [17,18] and developed the OM algorithm that computes a representation of the prime ideals $\mathfrak{p}$ dividing a prime $p \in A$ by way of factoring f over the p-adic completion of K. This led to an efficient computation of the local basis $\mathcal{B}_\mathfrak{p}$, last missing ingredient in Okutsu's strategy. This opened the door to various OM-based routines: methods of multipliers [1,3,11], method of the quotients [12] and finally the remarkably simple `MaxMin` algorithm of Stainsby [25] that we follow here.

Summary of our strategy. We do not claim any originality in our approach, following the classical local to global strategy outlined in [2,25]:

1. Run the fast OM algorithm [24] above each prime $p \in A$ dividing Δ (if we start with a squarefree factor, we rely on dynamic evaluation) and deduce for each prime ideal $\mathfrak{p} \subset B$ dividing p a local $\mathfrak{p}$-integral basis together with a suitable approximant of the associated local factor $F_\mathfrak{p}$ of f.
2. Apply the `MaxMin` algorithm [25] to deduce a triangular p-integral basis (each numerator being a suitable multiplicative combination of the numerators of the various $\mathfrak{p}$-bases).
3. Use the Chinese Reminder Theorem to glue these p-integral basis as a global triangular integral basis.

Concerning Point 2, it is remarkable that [25] allows to compute a *triangular* p-integral basis avoiding the usual costly Hermite type reduction step. The OM algorithm was the main bottleneck of the associated complexity analysis given in [26] and our improvements mainly follow from the recent faster OM algorithm [24], together with a careful study of the various p-adic precisions needed to conduct the computations.

Organisation of the paper. In Section 2, we first remind how local integral bases (one for each factor of the local factorisation of f) are deduced from the Okutsu frames computed during the OM algorithm. Then, we prove that the usual precision $v_p(\Delta)$ used in the OM algorithm can be improved by $2\,v_p(D)+1$, key result towards the proof of Theorem 1. Section 3 is dedicated to glue local bases into a reduced triangular p-integral basis thanks to the `MaxMin` algorithm of Stainsby, these p-integral bases being then glued into an integral basis of L/K using Chinese remaindering (Subsection 3.3). Section 4 is dedicated to integral bases of arbitrary fractional ideals. We pay attention to complexity issues and prove our main Theorem 1 in Section 5 . Finally, we illustrate the overall strategy with an example of [25] in Section 6.

2 OM algorithm and local integral basis

Let A be a principal ideal domain with field of fraction K and let $L = K(\theta)$ be the field extension determined by a root $\theta \in \overline{K}$ of a monic, irreducible and separable polynomial $f \in A[x]$ of degree d.

The OM algorithm [22], from the initial of its main artisans Ore, MacLane, Okutsu and Montes, computes an OM representation of each prime ideal of L lying over a given prime $p \in A$. This computational object supports several arithmetic data attached to an irreducible factor (say F) of f over the p-adic completion K_p of K. In particular, it allows to compute a local integral basis of the finite extension of K_p determined by F, first step towards the local-to-global computation of an integral basis of L/K. After recalling this construction, we give new tight bounds for the precision required by the OM algorithm.

2.1 Local integral basis and OM-factorisation.

We fix a prime $p \in A$ and consider $v_p : K^\times \to \mathbb{Z}$ the p-adic valuation, K_p the completion of K with respect to v_p and $\mathcal{O}_p$ the valuation ring of K_p. We still denote v_p the canonical extension of v_p to a fixed algebraic closure $\overline{K}_p$ of K_p.

Okutsu frame and local integral basis. Let $F \in \mathcal{O}_p[x]$ be an irreducible monic polynomial of degree n and let $\alpha \in \overline{K}_p$ be a root of F.

Definition 1. *An* Okutsu frame *of F is a sequence $[\phi_1, \ldots, \phi_{r+1}]$, with $\phi_i \in \mathcal{O}_p[x]$ monic of degree m_i such that (denoting $m_0 = 1$, $\phi_0 = 1$):*

- $m_1 \,|\, m_2 \,|\, \cdots \,|\, m_{r+1}$ *and* $1 \le m_1 < m_2 < \cdots < m_{r+1} = n$.
- *For all $g \in \mathcal{O}_p[x]$ monic,* $\deg g < m_{i+1} \Longrightarrow \frac{v_p(g(\alpha))}{\deg(g)} \le \frac{v_p(\phi_i(\alpha))}{m_i} < \frac{v_p(\phi_{i+1}(\alpha))}{m_{i+1}}$

The polynomial ϕ_{r+1} is called an Okutsu approximant *of F.*

The degrees $m_i = \deg(\phi_i)$ and the length r do not depend on the choice of the frame. For any $0 \le m < n$, we can write in a unique way $m = j_0\, m_0 + \cdots + j_r\, m_r$ with $0 \le j_i < m_{i+1}/m_i$. We accordingly let

$$g_m := x^{j_0} \phi_1^{j_1} \cdots \phi_r^{j_r} \in \mathcal{O}_p[x].$$

The integral closure $\overline{\mathcal{O}}_p$ of $\mathcal{O}_p$ in $K_p(\alpha)$ is a free $\mathcal{O}_p$-module of rank n. Okutsu proved [20, Theorem 1]:

Proposition 1. *Let $\eta_m = \lfloor v_p(g_m(\alpha)) \rfloor$. The family $1, \frac{g_1(\alpha)}{p^{\eta_1}}, \ldots, \frac{g_{d-1}(\alpha)}{p^{\eta_{d-1}}}$ is an $\mathcal{O}_p$-basis of $\overline{\mathcal{O}}_p$. We call it an* Okutsu basis *of F.*

We have $\eta_1 \le \cdots \le \eta_{d-1} = \exp(F)$ where $\exp(F)$ is the *integrality exponent* of F, least integer such that $p^{\exp(F)}\overline{\mathcal{O}}_p \subset \mathcal{O}_p[\alpha]$.

Definition 2. *Let $g_0 = 1$ and $g_n = \phi_{r+1}$. The set $\mathcal{N}(F) := \{g_0, g_1, \ldots, g_{n-1}, g_n\}$ is called an extended set of* Okutsu numerators *of F.*

OM-factorisation. The prime ideals $\mathfrak{p}$ of L dividing p are one-to-one with the irreducible monic factors of f in $\mathcal{O}_p[x]$. We denote $f = \prod_{\mathfrak{p}|p} F_\mathfrak{p}$ and we let $\theta_\mathfrak{p} \in \overline{K}_p$ be an arbitrary root of $F_\mathfrak{p}$.

Definition 3. *An Okutsu factorisation of f above p is a set $(\mathcal{F}_\mathfrak{p})_{\mathfrak{p}|p}$ where $\mathcal{F}_\mathfrak{p} := [\phi_{\mathfrak{p},0}, \ldots, \phi_{\mathfrak{p},r_\mathfrak{p}+1}]$ is an Okutsu frame of $F_\mathfrak{p}$, with $\phi_{\mathfrak{p},i} \in A[x]$. An OM-factorisation of f above p is an Okutsu factorisation s.t. the approximants $\phi_\mathfrak{p} := \phi_{\mathfrak{p},r_\mathfrak{p}+1}$ satisfy $v_p(\phi_\mathfrak{p}(\theta_\mathfrak{p})) > v_p(\phi_\mathfrak{p}(\theta_\mathfrak{q}))$ for all $\mathfrak{p} \neq \mathfrak{q}$ (see [4, Definition 3.2]).*

The stronger condition for being an OM-factorisation ensures that the approximant $\phi_\mathfrak{p}$ uniquely determines the corresponding factor $F_\mathfrak{p}$ of f (we might have $\phi_\mathfrak{p} = \phi_\mathfrak{q}$ for some $\mathfrak{q} \neq \mathfrak{p}$ in an Okutsu factorisation).

The fast OM algorithm of [24] will allow us to compute an OM-factorisation of f in the aimed complexity bound, together with all the $\phi_{\mathfrak{p},i}$ defined above, thus an Okutsu basis of each $F_\mathfrak{p}$ thanks to Proposition 1.

2.2 Precision of the OM algorithm

We improve here the results of [4] about the precision required for computing an OM-factorisation of f (and a p-integral basis). This section is quite technical, depending a lot of the references [4,19,24]. It is independent of the strategy for the computation of a triangular integral basis and the reader mainly interested on that part can skip it.

The Okutsu bound. For $F \in \mathcal{O}_p[x]$ monic, separable and irreducible, and α a root of F, we define the *Okutsu bound* of F as

$$\delta_0(F) := \deg(F)\ \max\left\{\frac{v_p(g(\alpha))}{\deg(g)},\ g \in \mathcal{O}_p[x] \text{ monic}, \deg(g) < d\right\}.$$

Given $f \in A[x]$ with irreducible factorisation $f = \prod_{\mathfrak{p}|p} F_\mathfrak{p} \in \mathcal{O}_p[x]$ as above, and denoting $d_\mathfrak{p} = \deg(F_\mathfrak{p})$, we let

$$\delta^*(f) := \frac{1}{2}\sum_{\mathfrak{p}|p} d_\mathfrak{p}\delta_0(F_\mathfrak{p}) + \sum_{\mathfrak{p}\neq\mathfrak{q}} v_p(Res(F_\mathfrak{p}, F_\mathfrak{q})).$$

In contrast to the discriminant valuation $\delta(f) := v_p(\Delta(f))$, the rational number $\delta^*(f)$ is an Okutsu invariant of f, that is it only depends on combinatorial data attached to an OM-factorisation f (see [19] for details). Both quantities are related by Proposition 2 below.

Bounds for $\delta^*(f)$. For each $\mathfrak{p}|p$, let $e_\mathfrak{p}$ and $f_\mathfrak{p}$ be respectively the ramification index and the residual degree of $\mathfrak{p}$ over p and let $L_\mathfrak{p} = K_p(\theta_\mathfrak{p})$. It is well known that $\Delta_{L_\mathfrak{p}/K_\mathfrak{p}}) \geq f_\mathfrak{p}(e_\mathfrak{p} - 1)$, with equality if and only if $L_\mathfrak{p}/K_p$ is tame, that is if $p \nmid e_\mathfrak{p}$ and the residue field extension is separable. We define

$$\rho(f) := \sum_{\mathfrak{p}|p} \left(v_p(\Delta_{L_\mathfrak{p}/K_\mathfrak{p}}) - f_\mathfrak{p}(e_\mathfrak{p} - 1)\right) \geq 0$$

which thus measures the non tameness of L/K.

Proposition 2. *We have* $\delta^*(f) \leq \delta(f) - \rho(f)$.

Proof. If $F \in \mathcal{O}_p[x]$ is monic irreducible with Okutsu frame $[\phi_1, \ldots, \phi_{r+1}]$, it follows from Definition 1 that $\delta_0(F) = \deg(F) v_p(\phi_r(\alpha))/\deg(\phi_r)$ and [4, Lemma 1.5] shows that $\delta_0(F)$ coincides with the quantity introduced in [4, Definition 2.1]. We thus get $\delta_0(F) = \mu_r + \nu_r \leq 2\mu_r =: 2\mu(F)$ where μ_r and ν_r are Okutsu invariants defined by the successive slopes of the generalised Newton polygon encountered during the OM algorithm called with parameter F (see [4, page 141]). Combined with [19, Proposition 1.4], we get for each $\mathfrak{p}|p$

$$\frac{d_\mathfrak{p}\delta_0(F_\mathfrak{p})}{2} \leq d_\mathfrak{p}\mu(F_\mathfrak{p}) = \delta(F_\mathfrak{p}) - f_\mathfrak{p}\rho_\mathfrak{p} \tag{3}$$

where $\rho_\mathfrak{p} \in \mathbb{N}$ is related to the local different by $v_\mathfrak{p}(\mathrm{Diff}(L_\mathfrak{p}/K_p)) = e_\mathfrak{p} - 1 + \rho_\mathfrak{p}$. Applying the norm $N_{L_\mathfrak{p}/K_p}$ and using that $\Delta_{L_\mathfrak{p}/K_p} = N_{L_\mathfrak{p}/K_p}(\mathrm{Diff}(L_\mathfrak{p}/K_p))$, we get $\sum_\mathfrak{p} f_\mathfrak{p}\rho_\mathfrak{p} = \rho(f)$. The claim follows from summing (3) over all $\mathfrak{p}|p$ together with the classical formula $\delta(f) = \sum_\mathfrak{p} \delta(F_\mathfrak{p}) + \sum_{\mathfrak{p}\neq\mathfrak{q}} v_p(\mathrm{Res}(F_\mathfrak{p}, F_\mathfrak{q}))$. □

The Okutsu invariant $\delta^*(f)$ is also closely related to the p-index. In what follows, we use notations

$$\mathrm{ind}_p(f) := v_p([B : A[\theta]]) \qquad \text{and} \qquad \mathrm{ind}_p(F_\mathfrak{p}) = v_p([B_\mathfrak{p} : A_p[\theta_\mathfrak{p}]]).$$

Thus $\mathrm{ind}_p(f) = v_p(D)$ with notations of the introduction.

Proposition 3. *We have the inequalities* $\mathrm{ind}_p(f) \leq \delta^*(f) \leq 2\,\mathrm{ind}_p(f) + d - 1$.

Proof. The first inequality follows from

$$\frac{d_\mathfrak{p}\delta_0(F_\mathfrak{p})}{2} \geq \frac{d_\mathfrak{p}}{2}\mu(F_\mathfrak{p}) = \mathrm{ind}_p(F_\mathfrak{p}) + 1 - e_\mathfrak{p}^{-1} \geq \mathrm{ind}_p(F_\mathfrak{p})$$

(the equality by [19, Proposition 1.4]) together with

$$\mathrm{ind}_p(f) = \sum_\mathfrak{p} \mathrm{ind}_p(F_\mathfrak{p}) + \frac{1}{2}\sum_{\mathfrak{p}\neq\mathfrak{q}} v_p(Res(F_\mathfrak{p}, F_\mathfrak{q}))$$

(see e.g. [19, Section 2.2]). For the second inequality, (2) leads to

$$\delta(f) = 2\,\mathrm{ind}_p(f) + v_p(\mathrm{Disc}(L/K)) = 2\,\mathrm{ind}_p(f) + \sum_{\mathfrak{p}|p} v_p(\mathrm{Disc}(L_\mathfrak{p}/K_\mathfrak{p})).$$

Combined with Proposition 2, we get $\delta^*(f) \leq 2\,\mathrm{ind}_p(f) + \sum_\mathfrak{p} f_\mathfrak{p}(e_\mathfrak{p} - 1)$ and we conclude thanks to the fundamental equality $\sum_{\mathfrak{p}|p} e_\mathfrak{p} f_\mathfrak{p} = d_\mathfrak{p}$. □

Theorem 2. *Let* $\sigma \in \mathbb{N}$ *and let* $g, f \in \mathcal{O}[x]$ *be two monic separable polynomials of degree* d *such that* $g \equiv f \mod p^\sigma$.

1. *If* $\sigma > 2\delta^*(f)/d$, *then* g *is irreducible if and only if* f *is irreducible.*
2. *If* $\sigma > \delta^*(f)$, *then any OM-factorisation of* g *is an OM-factorisation of* f.

Proof. Point 1 follows from a closer look at the proof of [4, Lemma 2.8]. Namely, the quantities $u_{i,s}/e_0 \cdots e_{i-1}$ that appear in the proof are upper bounded by $2\delta(F_s)/n_s$ (with $n_s = \deg(F_s)$) although [4, Lemma 2.2] allows to use the Okutsu bound to get a sharper inequality

$$\frac{u_{i,s}}{e_0 \cdots e_{i-1}} \leq \delta_0(F_s) \leq \frac{2\delta(F_s)}{n_s}.$$

Hence, we may replace $\delta(F_s)$ by $n_s\delta_0(F_s)/2$ in [4, inequalities (2.5) and (2.6)]. By definition of $\delta^*(f)$, we get that $\delta(f)$ can be replaced by $\delta^*(f)$ in the upper bound of [4, Lemma 2.8]. We may thus also use $\delta^*(f)$ instead of $\delta(f)$ in [4, inequality (2.8)] of the proof of [4, Theorem 2.3], leading to Point 1. Similarly, we may replace $\delta(f)$ by $\delta^*(f)$ in [4, Lemma 3.12], from which it follows that we may replace $\delta(f)$ by $\delta^*(f)$ in [4, Theorem 3.13], proving Point 2. □

Example 2. Consider $f = x^2 + t^N x + t \in F_2[[t]][x]$. We check that $\delta^*(f) = 1$ while $\delta(f) = 2N$ can take arbitrarily large values for the fixed degree $d = 2$. By Theorem 2, the OM-factorisation of f only depends on $f \mod p^2$, and we definitely don't want to work at precision $\delta(f) = 2N$ for such a polynomial.

In terms of the index, Theorem 2 together with Proposition 3 shows that we can work at precision $2\,\mathrm{ind}_p(f) + d$ to get an OM factorisation of f. In fact, we can do slightly better.

Theorem 3. *Let $\tilde{\delta}(f) := 2\,ind_p(f) + 1$. Let $g \in \mathcal{O}[x]$ be a monic separable polynomial of degree d such that $g \equiv f \mod p^\sigma$ for some $\sigma > \tilde{\delta}(f)$.*

1. *Any OM-factorisation of g is an OM-factorisation of f.*
2. *Running the OM algorithm of [24] with precision σ returns an OM-factorisation of f where the approximant $\phi_\mathfrak{p}$ of $F_\mathfrak{p}$ satisfy $v_p(F_\mathfrak{p} - \phi_\mathfrak{p}) > \sigma - ind_p(f)$.*
3. *The approximants $\phi_\mathfrak{p}$ satisfy the conditions of Corollary 3 of Section 3.*

Proof. The proof is algorithmic. We first call algorithm `Irreducible` of [24] with precision σ. By Proposition 3, we have $\tilde{\delta}(f) \geq 2\delta^*(f)/d$, so Theorem 2 ensures that either we can certify f that is irreducible (and compute in such a case an Okustsu approximant of f), or we detect a first partial factorisation that can be computed up to precision σ thanks to a valuated Hensel lemma, getting

$$f \equiv G_0 \cdots G_r \mod p^\sigma.$$

Each G_i can be lifted to a factor F_i of f (not necessarily irreducible). Denoting μ the current augmented valuation (denoted w in [24]) and e the current ramification index (which is $w(\pi)$ in [24]) we deduce from [24, Lemma 9] that

$$\sigma_i := v_p(G_i - F_i) \geq \sigma - \frac{\mu(G_i)}{e}.$$

Now, denoting $\hat{F}_i$ the cofactor of F_i in f, we deduce from [4, Proposition 3.5] $\frac{\mu(G_i)}{e} = \frac{\mu(F_i)}{e} = \frac{v(\mathrm{Res}(F_i, \hat{F}_i))}{deg(\hat{F}_i)} \leq v(\mathrm{Res}(F_i, \hat{F}_i))$. [19, Section 2.2] leads to $\mathrm{ind}_p(f) =$

$\mathrm{ind}_p(F_i)+\mathrm{ind}_p(\hat{F}_i)+v(\mathrm{Res}(F_i,\hat{F}_i))$. As by assumption $\sigma > 2\,\mathrm{ind}_p(f)+1$, we get

$$\sigma_i > \mathrm{ind}_p(f)+\mathrm{ind}_p(F_i)+\mathrm{ind}_p(\hat{F}_i)+1 \geq \mathrm{ind}_p(f)+\mathrm{ind}_p(F_i)+1.$$

As $\sigma_i > 2\,\mathrm{ind}_p(F_i)+1$, we can apply recursively this strategy on each approximant $G_i \equiv F_i \mod p^{\sigma_i}$, working now with precision σ_i. At a recursive call on an approximant G of a factor F of f, the current precision σ' satisfies

$$\sigma' \geq \sigma - \mathrm{ind}_p(f) > \mathrm{ind}_p(f)+\mathrm{ind}_p(F)+1 \geq 2\mathrm{ind}_p(F)+1 \geq 2\delta^*(F)/\deg(F)$$

so that the algorithm terminates and provides a complete OM-factorisation

$$f \equiv \prod_{\mathfrak{p}} G_{\mathfrak{p}} \mod \pi^{\sigma} \quad \text{with} \quad v_p(G_{\mathfrak{p}}-F_{\mathfrak{p}}) \geq \sigma - \mathrm{ind}_p(f) \quad \forall\ \mathfrak{p}|p.$$

This proves Points 1 and 2. In particular, we get $v_p(G_{\mathfrak{p}}-F_{\mathfrak{p}}) > \mathrm{ind}_p(f)+1$. Using notations of Corollary 3, we have $\mathrm{ind}_p(f) = \lfloor\alpha_1\rfloor + \cdots \lfloor\alpha_{d-1}\rfloor \geq \lfloor\alpha_{d-1}\rfloor$ so that $v_p(G_{\mathfrak{p}}-F_{\mathfrak{p}}) > \alpha_{d-1}$, proving Point 3. □

Example 3. For the example $f = x^q + t^q x + t \in \mathbb{F}_q[t][x]$ of the introduction of degree $d = q$ (a prime), we get $\delta(f) = d^2$, $\delta^*(f) = d-1$ and $\tilde{\delta}(f) = 1$: we gain an extra factor d for the precision when considering $\tilde{\delta}(f)$ rather than $\delta^*(f)$.

Remark 1. The bound $\sigma > 2\,\mathrm{ind}_p(f)+1$ is sharp at least when $\mathrm{ind}_p(f) = 0$. Consider for instance $f = \prod_{i=0}^{n}((x-i)^2-p)+p^N$ with $N >> 0$, satisfying $\mathrm{ind}_p(f) = 0$. Factoring $f \equiv \prod_i (x-i)^2 \mod p$ would be neither sufficient to compute an OM-factorisation nor to detect if $\mathrm{ind}_p(f) = 0$. Factorisation modulo p^2 is required (see also Lemma 5).

Remark 2. A closer look at the proof shows that a precision $2\max \delta^*(g)/\deg(g)$ is sufficient for computing an OM-factorisation, where the max runs over all monic factors (possibly reducible) $g \in \mathcal{O}_p[x]$ of f. In most cases (when the index is not mainly due to one factor of small degree), this leads to a much smaller precision $\mathcal{O}(\delta^*(f)/d)$, which belongs to $\mathcal{O}(\mathrm{ind}_p(f)/d)$ by Proposition 3. This is the case for instance in the example detailled in Section 6.

3 Triangular p-integral bases

We keep notations of Section 2. Let $B \subset L$ stands for the integral closure of A in L. Denote A_p the localisation of A at a fixed prime $p \in A$ and B_p the integral closure of A_p in L. We have $B_p = B \otimes_A A_p$ and B_p is a free A_p-module of rank $d = \deg(f)$.

Definition 4. *A p-integral basis of B/A (or p-basis) is an A_p-basis of B_p.*

There are several ways to compute a p-integral basis from the local basis $\mathcal{B}_{\mathfrak{p}}$ of the local rings $\mathcal{O}_{\mathfrak{p}}$ for all $\mathfrak{p}$ dividing p [5,11,12,3]. Traditional methods (based on the work of Okutsu [20]) compute a p-basis of shape $\mathcal{B}_p := \bigcup_{\mathfrak{p}|p} z_{\mathfrak{p}}\mathcal{B}_{\mathfrak{p}}$ for some

well chosen multipliers $z_{\mathfrak{p}} \in B_p$ (see also [12] for the method of the quotients). Although the complexity of such methods fit in our aimed complexity bound, the resulting p-basis is not triangular in general and the Hermite type reduction needed before applying CRT (Proposition 5) does not fit in our aimed complexity bound. The wonderful `MaxMin` algorithm of Stainsby [25] avoids this problem by providing directly a triangular p-integral basis.

3.1 Reduced triangular p-integral bases.

For any prime ideal $\mathfrak{p}$ dividing p, we define a valuation $w_{\mathfrak{p}} : L^{\times} \to \mathbb{Q}$ by

$$w_{\mathfrak{p}}(g(\theta)) := \frac{v_{\mathfrak{p}}(g(\theta))}{e_{\mathfrak{p}}}$$

where $e_{\mathfrak{p}} = e(\mathfrak{p}/p)$ is the ramification index and $v_{\mathfrak{p}}$ is the canonical discrete valuation attached to $\mathfrak{p}$. Thus $w_{\mathfrak{p}}$ extends v_p to L and $w_{\mathfrak{p}}(g(\theta)) = v_p(g(\theta_{\mathfrak{p}}))$ where $\theta_{\mathfrak{p}} \in \overline{K}_p$ is any root of $F_{\mathfrak{p}}$. Let $w = w_p$ be the quasi-valuation defined by

$$w : L \to \mathbb{Q} \cup \{\infty\}, \qquad w(b) := \min(w_{\mathfrak{p}}(b),\ \mathfrak{p}|p).$$

Thus, an element $b \in L$ belongs to B_p if and only if $w(b) \geq 0$.

Definition 5. *We say that a subset $\mathcal{B} = \{b_0, \ldots, b_k\} \subset L$ is* w-reduced *if $w(\sum_i \lambda_i b_i) = \min_i w(\lambda_i b_i)$ for all $\lambda_0, \ldots \lambda_k \in K$.*

Computing w-reduced integral bases is relevant for several applications in function fields, such as computing Riemann-Roch spaces [2, Section 5] (possibly using various quasi-valuations w). Given $g_0, \ldots, g_k \in A[x]$, we denote by

$$\mathcal{B}(g_0, \ldots, g_k) := \left(\frac{g_0(\theta)}{p^{\lfloor w(g_0(\theta)) \rfloor}}, \ldots, \frac{g_k(\theta)}{p^{\lfloor w(g_k(\theta)) \rfloor}} \right).$$

Definition 6. *A p-integral basis of shape $\mathcal{B}(g_0, \ldots, g_{d-1})$ with g_i monic of degree i is called a triangular p-basis.*

For all $i = 0, \ldots, d-1$, we define $\alpha_i = \alpha_i(f, p) \in \mathbb{Q}^+$ by

$$\alpha_i = \max \{ w(h(\theta)),\ h \in A[x] \text{ monic},\ \deg(h) = i \}. \tag{4}$$

We say that $g \in A[x]$ monic of degree i is *w-maximal* if $w(g(\theta)) = \alpha_i$.

Proposition 4. *[25, Theorem 1.4] Let $\mathcal{B} = \mathcal{B}(g_0, \ldots, g_{d-1})$, with g_i monic of degree i. Then*

- *$\mathcal{B}$ is a p-integral basis if and only if $\lfloor w(g_i(\theta)) \rfloor = \lfloor \alpha_i \rfloor$.*
- *$\mathcal{B}$ is a reduced p-integral basis if and only if $w(g_i(\theta)) = \alpha_i$.*

Corollary 2. *Let $\mathcal{B} = \mathcal{B}(g_0, \ldots, g_{d-1})$ and $\mathcal{B}' = \mathcal{B}(h_0, \ldots, h_{d-1})$, with $g_i, h_i \in A[x]$ monic of degree i. If $\mathcal{B}$ is a triangular (resp. reduced triangular) p-basis and $h_i \equiv g_i \mod p^{\lfloor \alpha_i \rfloor}$ (resp. $h_i \equiv g_i \mod p^{\lceil \alpha_i \rceil}$), then $\mathcal{B}'$ is a triangular (resp. reduced triangular) p-basis.*

Proof. Let $g, h \in A[x]$ and let $\alpha = w(g(\theta))$. If $h \equiv g \mod p^{\lfloor \alpha \rfloor}$ then $\lfloor w(h(\theta)) \rfloor = \lfloor \alpha \rfloor$ while if $h \equiv g \mod p^{\lceil \alpha \rceil}$ then $w(h(\theta)) = \alpha$. Proposition 4 concludes. □

By Proposition 4, computing a reduced triangular p-basis amounts to compute for each degree $i = 0, \dots, d-1$ a maximal monic polynomial $g_i \in A[x]$ of degree i. It is shown in [25] that such polynomials can be obtained as the product of exactly one Okutsu numerator of the local basis $\mathcal{B}_{\mathfrak{p}}$, for each $\mathfrak{p}|p$.

3.2 The `MaxMin` algorithm.

For each $\mathfrak{p}|p$, denote $d_{\mathfrak{p}} = \deg(F_{\mathfrak{p}})$ and consider an extended set of Okutsu $\mathfrak{p}$-numerators of $F_{\mathfrak{p}}$ (Definition 2)

$$\mathcal{N}_{\mathfrak{p}} := \mathcal{N}(F_{\mathfrak{p}}) = \{g_{\mathfrak{p},0}, \dots, g_{\mathfrak{p},d_{\mathfrak{p}}-1}, g_{\mathfrak{p},d_{\mathfrak{p}}} = \phi_{\mathfrak{p}}\}.$$

For each multi-index $\mathbf{j} = (j_{\mathfrak{p}})_{\mathfrak{p}|p}$ with $0 \le j_{\mathfrak{p}} \le d_{\mathfrak{p}}$, we define $g_{\mathbf{j}} := \prod_{\mathfrak{p}|p} g_{\mathfrak{p},j_{\mathfrak{p}}}$, so that $g_{\mathbf{j}} \in A[x]$ is monic of degree $\deg(\mathbf{j}) := \sum_{\mathfrak{p}|p} j_{\mathfrak{p}} \le d$.

Theorem 4. *[25, Theorem 2.6] If the approximants $\phi_{\mathfrak{p}}$ are computed with a sufficient precision, then there exists for each $i = 0, \dots, d-1$ a multi-index $\mathbf{j}_i$ of degree i such that $g_i := g_{\mathbf{j}_i}$ is maximal, i.e. $w(g_i(\theta)) = \alpha_i$.*

We want to look for such optimal multi-indices without taking care of the precision of the approximant $\phi_{\mathfrak{p}}$. To this aim, we rather consider $\phi_{\mathfrak{p}}$ as a symbol and use the map

$$w_{\mathfrak{p}}(g_{\mathbf{j}}) = \begin{cases} w_{\mathfrak{p}}(g_{\mathbf{j}}(\theta)) & \text{if } \phi_{\mathfrak{p}} \nmid g_{\mathbf{j}} \\ \infty & \text{if } \phi_{\mathfrak{p}} \mid g_{\mathbf{j}}. \end{cases}$$

Let accordingly $w(g_{\mathbf{j}}) := \min\{w_{\mathfrak{p}}(g_{\mathbf{j}}),\ \mathfrak{p}|p\}$. We have $w(g_{\mathbf{j}}) < \infty$ if $\deg(\mathbf{j}) < d$.

Definition 7. *We say that the multi-index $\mathbf{j}$ is maximal if $w(g_{\mathbf{j}}) \ge w(g_{\mathbf{i}})$ for all multi-index $\mathbf{i}$ with $\deg(\mathbf{i}) = \deg(\mathbf{j})$.*

Denote $\mathcal{P} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ the set of prime ideals of B dividing p in a given fixed order. Denote $(\mathbf{e}_1, \dots, \mathbf{e}_s)$ the canonical basis of $\mathbb{Z}^s$.

Algorithm: `MaxMin`$(\mathcal{N}_{\mathfrak{p}_1}, \dots, \mathcal{N}_{\mathfrak{p}_s})$
Input: A set $\mathcal{N}_{\mathfrak{p}_1}, \dots, \mathcal{N}_{\mathfrak{p}_s}$ of local Okutsu numerators of f.
Output: Some maximal multi-indices $\mathbf{j}_0, \dots, \mathbf{j}_{d-1}$ of degrees $0, \dots, d-1$.
1 $\mathbf{j}_0 \leftarrow (0, \dots, 0)$;
2 **for** $k = 0, \dots d-1$ **do**
3 $j \leftarrow \min\{1 \le i \le s,\ w_{\mathfrak{p}_i}(g_{\mathbf{j}_k}) = w(g_{\mathbf{j}_k})\}$;
4 $\mathbf{j}_{k+1} \leftarrow \mathbf{j}_k + \mathbf{e}_j$;

Theorem 5. *[25, Theorem 3.3] There exists an ordering on the set $\mathcal{P} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ such that algorithm* `MaxMin` *returns a correct answer.*

We say in such a case that $\mathcal{P}$ is well-ordered. Such an order can be read for free on the tree of types induced by the OM-factorisation of f, see [25, Section 3.2] for details. Note that despite of the remarkably simplicity of algorithm `MaxMin`, the proofs of Theorems 4 and 5 in [25] are quite involved.

Corollary 3. *Let $\mathbf{j}_0, \dots, \mathbf{j}_{d-1}$ be a sequence of maximal multi-indices, as returned by algorithm* `MaxMin` *(assuming $\mathcal{P}$ well-ordered). Denote $g_i := g_{\mathbf{j}_i}$. If the precision of the approximant satisfies $v_p(F_\mathfrak{p} - \phi_\mathfrak{p}) \geq \alpha_{d-1}$ for all $\mathfrak{p}|p$, then g_i is a degree i maximal polynomial for all $i = 0, \dots, d-1$. We have $w(g_i(\theta)) = \alpha_i$ and get the reduced triangular p-basis*

$$\mathcal{B} = \left(1, \frac{g_1(\theta)}{p^{\lfloor \alpha_1 \rfloor}}, \dots, \frac{g_{d-1}(\theta)}{p^{\lfloor \alpha_{d-1} \rfloor}}\right).$$

Proof. We have by the very definition

$$w(g_i) = \min\{w_\mathfrak{p}(g_i(\theta)),\ \mathfrak{p}|p, \phi_\mathfrak{p} \nmid g_i\} \geq \min\{w_\mathfrak{p}(g_i(\theta)),\ \mathfrak{p}|p\} = w(g_i(\theta)).$$

If strict inequality holds then necessarily $w(g_i(\theta)) = w_\mathfrak{p}(g_i(\theta))$ for some prime $\mathfrak{p}$ such that $\phi_\mathfrak{p}$ divides g_i, from which it follows that $w(g_i(\theta)) \geq w_\mathfrak{p}(\phi_\mathfrak{p}(\theta))$. On the other hand, we have $\alpha_i \geq w(g_i(\theta))$ by definition of α_i. We get $\alpha_i \geq w(g_i(\theta)) \geq w_\mathfrak{p}(\phi_\mathfrak{p}(\theta)) = v(\phi_\mathfrak{p}(\theta_\mathfrak{p})) = v((\phi_\mathfrak{p}(\theta_\mathfrak{p}) - F_\mathfrak{p}(\theta_\mathfrak{p})) \geq v_0(F_\mathfrak{p} - \phi_\mathfrak{p}) \geq \alpha_{d-1}$. Since $\alpha_{d-1} \geq \alpha_i$, this forces $w(g_i(\theta)) = \alpha_i$ and we conclude with Proposition 4. Suppose now that equality $w(g_i) = w(g_i(\theta))$ holds. By Theorem 4, there is some $g = g_\mathbf{i}$ of degree i such that $w(g(\theta)) = \alpha_i$ (up to compute the $\phi_\mathfrak{p}$'s with high enough precision). As $\mathbf{j}_i$ is maximal, we have $w(g) \leq w(g_i)$ independently of the chosen precision. We get $w(g_i(\theta)) = w(g_i) \geq w(g) \geq w(g(\theta)) = \alpha_i \geq w(g_i(\theta))$, the last inequality by definition of α_i. Again, this forces $w(g_i(\theta)) = \alpha_i$. □

3.3 Global integral bases

For each prime $p \in A$, we saw how to compute a (reduced) p-integral basis

$$\mathcal{B}_p = \left(1, \frac{g_{p,1}(\theta)}{p^{\eta_{p,1}}}, \dots, \frac{g_{p,d-1}(\theta)}{p^{\eta_{p,d-1}}}\right)$$

with $g_{p,i} \in A[x]$ monic of degree i and $\eta_{p,i} = \lfloor w_p(g_{p,i}(\theta)) \rfloor$. We can glue these various p-bases to get a triangular integral basis thanks to the following result, due to Okutsu [21, Thm 1] (see also [26, Thm 1.17] or [2, Lem 1.3.18]):

Proposition 5. *Suppose given a p-basis $\mathcal{B}_p$ as above for each prime $p \,|\, D_f$. For all $i = 0, \dots, d-1$, let $h_i \in A[x]$ monic of degree i such that $h_i \equiv g_{p,i} \bmod p^{\eta_{p,i}+1}$ for all $p \,|\, D_f$. Then, the following family is a triangular integral basis of L/K:*

$$\mathcal{B} = \left(1, \frac{h_1(\theta)}{\prod_p p^{\eta_{p,1}}}, \dots, \frac{h_{d-1}(\theta)}{\prod_p p^{\eta_{p,d-1}}}\right).$$

4 Bases of fractional ideals

4.1 Fractional ideals

We keep notations and hypothesis of the previous section. Recall that any fractional ideal I of B is a free A-module of rank d.

Definition 8. *A triangular basis (with respect to f) of a fractional ideal I of B is an A-basis of I of shape*

$$\mathcal{B}_I = \left(\frac{1}{a_0}, \frac{g_1(\theta)}{a_1}, \dots, \frac{g_{d-1}(\theta)}{a_{d-1}} \right), \tag{5}$$

where $a_i \in K^\times$ satisfy $a_{d-1}A \subset \cdots \subset a_0 A$ and $g_i \in A[x]$ is monic of degree i.

Any fractional ideal admits a triangular basis [26, Theorem 1.16]. The fractional ideals $a_i A$ of A depend on the choice of f used to represent the field L/K but the first fractional ideal $a_0 A$ does not:

Lemma 1. *We have $a_0^{-1}A = I \cap K$.*

Proof. Let $\mathcal{B}_I = (b_0, \dots, b_{d-1})$ be a triangular basis of I and let $\alpha \in I$. Hence $\alpha = \sum \alpha_i b_i$ for some uniquely determined $\alpha_i \in A$. We have $\alpha \in K$ if and only if α has degree zero as a polynomial in θ. Since $\mathcal{B}_I$ is triangular, this is equivalent to $\alpha_1 = \cdots = \alpha_{d-1} = 0$. Hence $I \cap K = b_0 A = a_0^{-1} A$. □

Definition 9. *With notations as above, we define the normalised ideal of I as $I^* := a_0 I$. We say that I is normalised if $I^* = I$.*

Notice that $1 \in I^*$ so that $B \subset I^*$. If $\mathcal{B}$ is a (triangular) integral basis of I^*, then obviously $a_0^{-1}\mathcal{B}$ is a (triangular) integral basis of I, and we may focus on the computation of an A-basis of a normalised ideal.

In all what follows, we will assume that we are given the unique factorisation of I in terms of the prime ideals of B, denoted by $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$, $n_\mathfrak{p} \in \mathbb{Z}$. There are efficient algorithms to determine such a factorisation given the OM-factorisations of f above the involved primes $p \in A$ [11].

The normalised ideal I^* is then easily deduced. Let $\mathcal{P}_A$ be the set of primes of A (*i.e.* a set of generators of the prime ideals of A). For $p \in \mathcal{P}_A$, we define

$$m_p = m_p(I) := \max \left\{ \left\lceil \frac{n_\mathfrak{p}}{e_\mathfrak{p}} \right\rceil, \ \mathfrak{p} | p \right\} \in \mathbb{Z}. \tag{6}$$

Lemma 2. *We have $v_p(a_0) = -m_p$ and $I^* = \prod_{p \in \mathcal{P}_A} \prod_{\mathfrak{p}|p} \mathfrak{p}^{n_\mathfrak{p} - e_\mathfrak{p} m_p}$.*

Proof. As $B \subset I^*$, we have $v_\mathfrak{p}(I^*) \leq 0$ for all $\mathfrak{p}$. This implies that $v_\mathfrak{p}(a_0) \leq -n_\mathfrak{p}$. If $\mathfrak{p}|p$, then $v_\mathfrak{p}(a_0) = e_\mathfrak{p} v_p(a_0)$, hence $-v_p(a_0) \geq n_\mathfrak{p}/e_\mathfrak{p}$. Since $v_p(a_0) \in \mathbb{Z}$ we deduce that $-v_p(a_0) \geq m_p$. If strict inequality holds for some p, we get

$$-v_p(a_0) \geq m_p + 1 \quad \Longrightarrow \quad -v_p(a_0) e_\mathfrak{p} \geq n_\mathfrak{p} e_\mathfrak{p} + e_\mathfrak{p} \quad \forall\ \mathfrak{p}|p,$$

and $-v_\mathfrak{p}(p a_0) \geq n_\mathfrak{p}$ for all $\mathfrak{p}$. This implies $(a_0 p)^{-1} \in I \cap K$ in contradiction with Lemma 1. Hence $v_p(a_0) = -m_p$ for all p and $v_\mathfrak{p}(I^*) = n_\mathfrak{p} - e_\mathfrak{p} m_p$ for all $\mathfrak{p}|p$. □

Normalised size of fractional ideals. Given two free A-submodules $I, I' \subset L$ of rank d with respective A-basis $\mathcal{B} = (b_1, \ldots, b_d)$ and $\mathcal{B}' = (b'_1, \ldots, b'_d)$, the transition matrix $T \in K^{d\times d}$ from $\mathcal{B}$ to $\mathcal{B}'$ is defined by $(b'_1, \ldots, b'_d)T = (b_1, \ldots, b_d)$. If we change the A-basis of I or I', then T is multiplied by a matrix in $GL_d(A)$. Hence the following definition makes sense :

Definition 10. *For two free A-submodules $I, I' \subset K$ of rank d, the index $[I' : I]$ is the fractional ideal of A generated by the determinant of the transition matrix from an A-basis of I to an A-basis of I'.*

The index is multiplicative : $[I : I''] = [I : I'][I' : I'']$. Moreover, if $I' \subset I$, then $[I : I'] \subset A$ and $I' = I$ if and only if $[I : I'] = A$.

If I has triangular basis as in Definition 8, then $[I : A[\theta]] = (a_0 \cdots a_{d-1})$ and by transitivity of the index, we get

$$v_p([I^* : A[\theta]]) = v_p(a_0 \cdots a_{d-1}) - dv_p(a_0) \ \geq 0,$$

positivity since $a_i A \subset a_0 A$.

Definition 11. *Suppose either $A = \mathbb{Z}$ and $h(p) := \log |p|$, or $A = k[t]$ and $h(p) := \deg(p)$. The* normalised size *of I is*

$$h(I) := \sum_{p\in\mathcal{P}_A} v_p([I^* : A[\theta]])\, h(p) \ \in \mathbb{N}.$$

Lemma 3. *Denote $D = D_f$ as in (2). Let I be a fractional ideal of B. Then $h(I) \geq h(D)$ and equality holds if and only if $I = \alpha B$ for some $\alpha \in K \setminus \{0\}$.*

Proof. We have $[I^* : A[\theta]] = [I^* : B][B : A[\theta]]$ and $v_p([B : A[\theta]]) = v_p(D)$ so that $v_p([I^* : A[\theta]]) = v_p([I^* : B]) + v_p(D)$. Since $B \subset I^*$, we have $v_p([I^* : B]) \geq 0$, leading to $h(I) \geq h(D)$. Equality is equivalent to that $v_p([I^* : B]) = 0$ for all prime p, that is $[I^* : B] = A$. Since $B \subset I^*$, this is equivalent to that $I^* = B$, proving the last claim. □

4.2 p-bases of fractional ideals

Let us fix $p \in A$ a prime. Denote $I_p := I \otimes_A A_p$ the localisation of I at p. Note that

$$I_p = \{b \in L, \ \ v_{\mathfrak{p}}(b) \geq n_{\mathfrak{p}} \ \ \forall\, \mathfrak{p}|p\}$$

and I_p is a fractional ideal of B_p. As such, it is a free A_p-module of rank d. A p-basis of I is by definition an A_p-basis of I_p. To compute such a basis, we can follow exactly the same strategy than for the case $I_p = B_p$, except that we consider now the shifted valuations

$$w_{\mathfrak{p},I} : L \to \mathbb{Q} \cup \{\infty\}, \qquad w_{\mathfrak{p},I}(b(\theta)) := w_{\mathfrak{p}}(b(\theta)) - \frac{n_{\mathfrak{p}}}{e_{\mathfrak{p}}}$$

and accordingly the map $w_I = w_{p,I}$ defined by

$$w_I : L \to \mathbb{Q} \cup \{\infty\}, \qquad w_I(b(\theta)) = \min(w_{\mathfrak{p},I}(b(\theta)),\ \mathfrak{p}|p).$$

Thus, an element $b \in L$ belongs to I_p if and only if $w_I(b) \geq 0$. Given $g_0, \ldots, g_k \in A[x]$, we denote by

$$\mathcal{B}_I(g_0, \ldots, g_k) := \left(\frac{g_0(\theta)}{p^{\lfloor w_I(g_0(\theta)) \rfloor}}, \ldots, \frac{g_k(\theta)}{p^{\lfloor w_I(g_k(\theta)) \rfloor}} \right).$$

Definition 12. *A triangular p-basis of I is a basis of shape $\mathcal{B}_I(g_0, \ldots, g_{d-1})$ with g_i monic of degree i.*

We let $\alpha_{I,i} = \max\{w(h(\theta)),\ h \in A[x] \text{ monic},\ \deg(h) = i\}$ for $i = 0, \ldots, d-1$ and say that $g \in A[x]$ monic of degree i is w_I-maximal if $w_I(g(\theta)) = \alpha_{I,i}$.

Theorem 6. *Suppose I normalised. Let $\mathbf{j}_0, \ldots, \mathbf{j}_{d-1}$ be a sequence of maximal multi-indices, as returned by Algorithm* `MaxMin` *called with the map w_I instead of w (assuming $\mathcal{P}$ well-ordered). Let $g_i := g_{\mathbf{j}_i}$. If $v_p(F_\mathfrak{p} - \phi_\mathfrak{p}) \geq \alpha_{I,d-1}$ for all $\mathfrak{p}|p$, then $\mathcal{B}_I(g_0, \ldots, g_{d-1})$ is a triangular p-basis of I.*

Proof. It follows from respectively [26, Theorems 1.25], [26, Theorem 5.1] and [26, Proposition 5.2] that the analogous of respectively Proposition 4, Theorem 4 and Theorem 5 still hold if we replace w by w_I and α_i by $\alpha_{I,i}$. This mainly follows from the fact that the valuations $w_{\mathfrak{p},I}$ are simply a shift of the valuations $w_\mathfrak{p}$. Since $I = \prod \mathfrak{p}^{n_\mathfrak{p}}$ is assumed to be normalised, we have $B \subset I$ hence $n_\mathfrak{p} \leq 0$ for all $\mathfrak{p}$. Thus, [26, Theorem 5.3] ensures that the analogous of Corollary 2 holds too if we replace w by w_I and α_i by $\alpha_{I,i}$. The proof of Theorem 6 is then *mutatis mutandi* identical to the proof Corollary 3. □

4.3 Improvements *via* S-basis

Let $S \subset \mathcal{P}$. For $b \in L$, define $w_{I,S}(b) = \min(w_{\mathfrak{p},I}(b),\ \mathfrak{p} \in S)$. If we apply algorithm `MaxMin` with the set of denominators $\{\mathcal{N}_\mathfrak{p}, \mathfrak{p} \in S\}$ as input and with $w_{I,S}$ instead of w, we get a family of multi-indices $\mathbf{j}_0, \ldots, \mathbf{j}_{d_S-1}$ with $\mathbf{j}_i = (\mathbf{j}_{i,\mathfrak{p}})_{\mathfrak{p} \in S}$, and where $d_S := \sum_{\mathfrak{p} \in S} \deg(F_\mathfrak{p})$. The resulting polynomials $g_i := g_{\mathbf{j}_i}$ have maximal $w_{S,I}$-valuation (assuming that the involved $\phi_\mathfrak{p}$ are computed with a sufficient precision) and give rise to a triangular set

$$\mathcal{B}_{I,S} := \left(\frac{g_0(\theta)}{p^{\lfloor w_{I,S}(g_0(\theta)) \rfloor}}, \ldots, \frac{g_{d_S-1}(\theta)}{p^{\lfloor w_{I,S}(g_{d_S-1}(\theta)) \rfloor}} \right)$$

that we call *an S-basis of I*. Besides playing a key role in the proof of the Theorem 5 in [25], these S-bases are also relevant to accelerate the computation of a triangular p-basis of I in some particular cases. In what follows we let

$$T = \left\{ \mathfrak{p} \in \mathcal{P}\,,\ \operatorname{ind}_p(F_\mathfrak{p}) = v_p(\operatorname{Res}(F_\mathfrak{p}, \hat{F}_\mathfrak{p})) = n_\mathfrak{p} = 0 \right\} \tag{7}$$

and we denote $S = \mathcal{P} \setminus T$.

Proposition 6. *Suppose I normalised. Let $g = \prod_{\mathfrak{p}\in T} \phi_{\mathfrak{p}} \in A[x]$ and consider $\mathcal{B}_{I,S} = (b_0, b_1, \ldots, b_{d_S-1})$ an S-basis of I as above. The set*

$$\mathcal{B}_I = (1, \theta, \ldots, \theta^{d-d_S-1}, g\, b_0, , \ldots, g\, b_{d_S-1})).$$

is a triangular p-integral basis of I.

Proof. Note first that $\deg(g) = d - d_S$ so the set $\mathcal{B}_I$ is indeed triangular. By Proposition 4 (in the context of fractionary ideals), we need to show that the polynomials x^i and gb_j are $\lfloor w_I \rfloor$-maximal for $0 \le i < \deg(g)$ and $0 \le j < d_S$. Let b be a w_I-maximal polynomial of degree $k < d$. By Theorem 4 (which remains valid with w_I instead of w), we may take $b = \prod_{\mathfrak{p}\in\mathcal{P}} b_{\mathfrak{p}}$, with $b_{\mathfrak{p}} \in \mathcal{N}_{\mathfrak{p}}$.

- If there exists $\mathfrak{p} \in T$ such that $b_{\mathfrak{p}} \neq \phi_{\mathfrak{p}}$, then $\deg(b_{\mathfrak{p}}) < d_{\mathfrak{p}}$, which forces $\lfloor w_{\mathfrak{p}}(b_{\mathfrak{p}}) \rfloor \le \mathrm{ind}_p(F_{\mathfrak{p}})$ (Proposition 1), hence $\lfloor w_{I,\mathfrak{p}}(b_{\mathfrak{p}}) \rfloor = 0$ since $\mathrm{ind}_p(F_{\mathfrak{p}}) = n_{\mathfrak{p}} = 0$. But $v_p(\mathrm{Res}(F_{\mathfrak{p}}, \hat{F}_{\mathfrak{p}})) = 0$ implies also that $w_{I,\mathfrak{p}}(b_{\mathfrak{q}}) = 0$ for all $\mathfrak{q} \neq \mathfrak{p}$. Hence $\lfloor w_{I,\mathfrak{p}}(b) \rfloor = 0$. As I is normalised, we have $\lfloor w_{I,\mathfrak{q}}(b) \rfloor \ge 0$ for all $\mathfrak{q}$ and we deduce $\lfloor w_I(b) \rfloor = 0$. As b is w_I-maximal, we deduce that $\lfloor \alpha_{I,k} \rfloor = 0$ and any monic degree k polynomial (in particular x^k) is $\lfloor w_I \rfloor$-maximal.
- If $b_{\mathfrak{p}} = \phi_{\mathfrak{p}}$ for all $\mathfrak{p} \in T$, then $b = gb'$ with $b' = \prod_{\mathfrak{p}\in S} b_{\mathfrak{p}}$. In particular, we have $k \ge \deg(g)$. We get

$$w_I(b) = \min_{\mathfrak{p}\in\mathcal{P}}(w_{I,\mathfrak{p}}(b') + w_{\mathfrak{p}}(g)) = \min_{\mathfrak{p}\in S}(w_{I,\mathfrak{p}}(b') + w_{\mathfrak{p}}(g)) = \min_{\mathfrak{p}\in S} w_{I,\mathfrak{p}}(b') = w_{I,S}(b'),$$

the second equality because $w_{\mathfrak{p}}(g) = \infty$ for $\mathfrak{p} \in T$ and the third equality because $v_p(\mathrm{Res}(F_{\mathfrak{q}}, \hat{F}_{\mathfrak{q}})) = 0$ for all $\mathfrak{q} \in T$ forces $w_{\mathfrak{p}}(g) = 0$ for all $\mathfrak{p} \in S$. Hence b is w_I-maximal if and only if b' is $w_{I,S}$-maximal and the claim follows. □

Remark 3. The basis $\mathcal{B}_I$ of Proposition 6 is not necessarily w_I-reduced (Definition 5). Consider for instance $f = (x-1)^2 + p \in A[x]$ and $I = B$. We have $\mathrm{ind}_p(f) = 0$ and using Proposition 6 would lead to the p-integral basis $\mathcal{B} = (1, \theta)$. This basis is not w-reduced as $w(\theta) = 0 < w(\theta - 1) = 1/2$. Using Corollary 3 would have returned the *reduced* p-basis $(1, \theta - 1)$.

4.4 Global triangular bases of fractional ideals

Proposition 7. *Let I be a normalised fractional ideal of L. Suppose given a triangular p-basis $\mathcal{B}_{I,p} = \mathcal{B}_{I,p}(g_{p,0}, \ldots, g_{p,d-1})$ of I for each prime p dividing $[I : A[\theta]]$ and let $\eta_{p,i}(I) := \lfloor w_I(g_{p,i}(\theta)) \rfloor$. For all $i = 0, \ldots, d-1$, let $h_i \in A[x]$ monic of degree i s.t. $h_i \equiv g_{p,i} \mod p^{\eta_{p,i}(I)+1}$ for all p dividing $[I : A[\theta]]$. Then a triangular A-basis of I is given by*

$$\mathcal{B}_I = \left(1, \frac{h_1(\theta)}{\prod_p p^{\eta_{p,1}(I)}}, \ldots, \frac{h_{d-1}(\theta)}{\prod_p p^{\eta_{p,d-1}(I)}}\right).$$

Proof. This follows from [26, Theorem 1.27], where we use moreover that $g_{p,0} = 1$ for all p since I is assumed to be normalised. □

Remark 4. If I is not normalised, we first compute I^* following Lemma 2 and then compute an integral basis $\mathcal{B}_{I^*}$ of I^* following Proposition 7. An integral basis of I is then given by $\mathcal{B}_I = \alpha\mathcal{B}_{I^*}$, with $\alpha := \prod_{p|[I^*:A[\theta]]} p^{m_p}$, the integer m_p being defined in (6).

Theorem 7. *Let I be a fractional ideal. Given a squarefree factorisation of the ideal $[I^* : A[\theta]]$, we can compute a triangular integral basis of I with*

1. *$\mathcal{O}_\epsilon(d\,h(I))$ operations in k if $A = k[t]$ with $char(k) = 0$ or $char(k) > d$,*
2. *$\mathcal{O}_\epsilon(d\,h(I) + h_D^2)$ operations in k if $A = k[t]$ with $char(k) \leq d$,*
3. *$\mathcal{O}_\epsilon(d\,h(I) + h_D^2)$ word operations if $A = \mathbb{Z}$.*

This result has to be compared to $\mathcal{O}_\epsilon(d^3\,h(I)^2 + d\,h_\Delta^2)$ that can be deduced from [2, Thm 5.3.19]. The proof will be given at the end of Section 5.

Remark 5. Note that when $I = B$, we get $h(B) = h_D$ so the first statement of Theorem 1 is a particular instance of Theorem 7.

Remark 6. We don't take into account the last multiplications inherent to the relation $\mathcal{B}_I = \alpha\mathcal{B}_{I^*}$ in our estimation cost. For many purposes, this step would lose crucial information.

5 Complexity and proofs of the main results

We keep notations and hypothesis of previous sections. In particular, $f \in A[x]$ is an irreducible separable monic degree d polynomial. For a prime $p \in A$, we denote k_p the residue field of $\mathcal{O}_p$ and we charge one operation in k_p for one operation in a fixed set $\mathcal{A} \subset A$ of representatives of k_p.

Cost of the OM-factorisation.

Proposition 8. *Assume $\sigma \geq 2\,\mathrm{ind}_p(f) + 1$. We can compute an OM factorization of f above p such that $v_p(\phi_\mathfrak{p} - F_\mathfrak{p}) \geq \sigma - \mathrm{ind}_p(f)$ for all $\mathfrak{p}|p$ with $\mathcal{O}_\epsilon(d\,\sigma)$ operations in k_p if $char(k_p) = 0$ or $> d$, and $\mathcal{O}_\epsilon(d\,\sigma + \mathrm{ind}_p(f)^2)$ operations in k_p otherwise. The algorithm returns as a byproduct the values $w_\mathfrak{q}(\phi_{\mathfrak{p},i}(\theta))$ for all $\mathfrak{p},\mathfrak{q}|p$ and all $0 \leq i \leq r_\mathfrak{p} + 1$.*

Proof. When $\mathrm{char}(k_p)$ is zero or $> d$, this follows from Theorem 3 together with [24, Thm 4]. When $0 < \mathrm{char}(k_p) < d$, the number of refinement steps inherent to the OM algorithm is bounded by $\mathcal{O}(\mathrm{ind}(f)/\ell_0)$ thanks to [10, Def 4.15 and Thm 4.18], with ℓ_0 being the first residual degree as used in [24, Lemma 4]. We thus need to add a cost $\tilde{\mathcal{O}}(\delta^*\,\mathrm{ind}_p(f))$ thanks to [24, Section 3] (replacing again δ by δ^* in [24, Thm 2]). By Proposition 3, this is $\tilde{\mathcal{O}}(\mathrm{ind}_p(f)^2 + d\,\mathrm{ind}_p(f))$ which fits in the aimed bound. □

Note that we only compute the square-free factorisation of the various residual polynomials and we rely on dynamic evaluation, using the complexity results of [16] in that context (see [24, Section 5.4]).

Binary cost of the `MaxMin` *algorithm.* We consider the general context of a normalised fractional ideal I of B. Denote for short $\mathrm{ind}_p(I) = v_p(I : A[\theta])$. Note that $\mathrm{ind}_p(B) = \mathrm{ind}_p(f) = v_p(D)$.

Proposition 9. *The cost of* `MaxMin` *above a prime p with respect to the quasi-valuation w_I is $\mathcal{O}(ds\log(\mathrm{ind}_p(I)))$ word operations, with s the number of irreducible factors of f in $\mathcal{O}_p[x]$.*

Proof. There are d iterations including one minimum of a set of cardinality s and one addition, each element having binary size bounded by $\log(\mathrm{ind}_p(I))$. □

With regards to Theorem 7, we need to take care that we might have $s > \mathrm{ind}_p(I)$. For such a small p-index, we rather use Proposition 6.

Lemma 4. *Suppose I normalised and let $S \subset \mathcal{P}$ as defined by (7). The binary cost of* `MaxMin` *to compute an S-basis of I is $\tilde{\mathcal{O}}(d\,\mathrm{ind}_p(I))$.*

Proof. The cost of `MaxMin` restricted to S is now $\mathcal{O}(d_S\,\mathrm{Card}(S)\,\log(\mathrm{ind}_p(I)))$. We have $\mathrm{ind}_p(I) = v_p([B : A[\theta]) + v_p([I : B]) = \mathrm{ind}_p(f) - v_p(N_{L/K}(I))$, leading to

$$\mathrm{ind}_p(I) = \sum_{\mathfrak{p}|p}\left(\mathrm{ind}_p(F_\mathfrak{p}) + \frac{1}{2}v_p(\mathrm{Res}(F_\mathfrak{p}, \hat{F}_\mathfrak{p}) - f_\mathfrak{p}n_\mathfrak{p}\right).$$

Since I is normalized, we have $n_\mathfrak{p} \leq 0$ for all p so each summand is $\geq 1/2$ whenever $\mathfrak{p} \in S$ by (7). We get $\mathrm{Card}(S) \leq \mathrm{ind}_p(I)/2$ and the claim follows. □

Cost of expanding and gluing p-integral basis.

Proposition 10. *Suppose I normalised. Up to the cost of the OM-factorisation, one can compute a triangular p-basis of I in less than $\tilde{\mathcal{O}}(d\,\mathrm{ind}_p(I))$ operations in k_p.*

Proof. Up to use Proposition 6 and Lemma 4, we can compute non expanded denominators $g_0, \ldots, g_{d-1}$ of a triangular p-basis $\mathcal{B}_I$ in the aimed cost (binary cost for this step). There remains to expand $g_i \bmod p^{\lfloor \alpha_{I,i}\rfloor}$ (Corollary 2 and Corollary 3 in the context of triangular ideal), for a cost of $\tilde{\mathcal{O}}(\deg(g_i)\lfloor\alpha_{I,i}\rfloor)$ operations in k_p. As $\sum_i \lfloor\alpha_{I,i}\rfloor = \mathrm{ind}_p(I)$ and $\deg(g_i) = i \leq d$, the total cost is $\tilde{\mathcal{O}}(d\,\mathrm{ind}_p(I))$ operations in k_p. □

Proposition 11. *Suppose I normalised. Given a triangular p-integral basis above each prime $p \in A$ dividing $[I : A[\theta]]$, we can compute a global integral basis of I in less than $\tilde{\mathcal{O}}(dh(I))$ binary operations if $A = \mathbb{Z}$ or $\tilde{\mathcal{O}}(dh(I))$ operations in k if $A = k[t]$.*

Proof. Let us first suppose that $A = k[t]$. Computing the polynomial $h_i \in A[x]$ in Proposition 7 requires $\tilde{\mathcal{O}}(\deg(h_i)\sum_p \eta_{p,i}(I)h(p))$ operations in k by fast Chinese multi-remaindering. The result follows by summing over all $i = 0, \ldots, d-1$, using $\deg(h_i) = i \leq d$, $\sum_{i=0}^{d-1}\eta_{p,i}(I) = \mathrm{ind}_p(I)$ and $\sum_p \mathrm{ind}_p(I)h(p) = h(I)$. The same reasonning applies if $A = \mathbb{Z}$, counting now the number of word operations. □

Proof of Theorem 7. We may assume $I = I^*$. By Theorem 6, it's enough to compute the $\phi_{\mathfrak{p}}$'s with precision $\mathrm{ind}_p(I)$. By Proposition 8, we may apply the OM algorithm with precision $\sigma = \mathrm{ind}_p(I)+\mathrm{ind}_p(f)+1$, which costs $\mathcal{O}_\epsilon(d\,\mathrm{ind}_p(I))$ operations in k_p (recall that $\mathrm{ind}_p(I) \geq \mathrm{ind}_p(f)$ since I is normalized), plus an extra $\mathcal{O}_\epsilon(\mathrm{ind}_p(f)^2)$ for small residual characteristic. The result then follows from Proposition 8, Proposition 10 and Proposition 11. Note that we rely again on dynamic evaluation since we are working above a squarefree factor p of the index of I which is not necessarily irreducible. □

Proof of Theorem 1. First part of Theorem 1 follows from Theorem 7 applied with $I = B$. Let us prove the last claim, assuming now that we only know a squarefree factorisation of the discriminant Δ. We use the following lemma.

Lemma 5. *Given a prime p, the condition $p|D$ only depends on $f \mod p^2$, and can be checked with $\mathcal{O}^{\sim}(d)$ operations in k_p.*

Proof. We want to check if $\mathrm{ind}_p(f) = 0$. We first compute the square-free factorisation of $f \mod p$ and lift it once to get $f = \prod_i F_i \mod p^2$, where $F_i|f$ and the F_i's are coprime mod p. This costs $\mathcal{O}^{\sim}(d)$ operations in k. We have $\mathrm{ind}_p(f) = 0$ if and only if $\mathrm{ind}_p(F_i) = 0$ for all i. Since $F_i = P_i^{N_i} \mod p$ with $P_i \in A[x]$ monic and square-free mod p, we have $\mathrm{ind}_p(F_i) = 0$ if and only if $N_i = 1$ or $v_p(F_i \mod P_i) = 1$ (Eisenstein case), see e.g. [10, Rem 4.13]. Both conditions only depend on $F_i \mod p^2$ and can be checked with $\mathcal{O}^{\sim}(\deg(F_i))$ operations in k_p for each i, hence a total cost $\mathcal{O}^{\sim}(d)$. □

The last claim in Theorem 1 follows. By (2), we need to check if $p|D$ only if $p^2|\Delta$. By Lemma 5, this adds an extra cost of $\mathcal{O}^{\sim}(d \sum_{p^2|\Delta} h(p)) = \mathcal{O}^{\sim}(dh_{red})$ (binary cost if $A = \mathbb{Z}$ or arithmetic cost if $A = k[t]$). □

6 An illustrative example

We conclude our paper by illustrating the different steps of our algorithm on the following example of Stainsby [25, Section 3.3] over $\mathbb{Z}[x]$, that is the polynomial

$$f = x^{13} + 3\,q^8\,x^{11} + 18753\,q^{12}\,x^{10} + 781253\,q^{16}\,x^9 + 244178131\,q^{20}\,x^8 + 783631254\,q^{24}\,x^7 + 14894940628\,q^{28}\,x^6 + 763967225003\,q^{32}\,x^5 + 193053764471876\,q^{36}\,x^4 + 1562575008\,q^{48}\,x^3 + 488318756\,q^{52}\,x^2 + 1527929762506\,q^{56}\,x + 4579209021877\,q^{60}$$

with $q = 5$. We have $\Delta_f = 2^6\,5^{744}\,n$ with n squarefree, and $D_f = 2^3\,5^{372}$. Knowing either of them, we first compute integral bases over $p = 2$ and $p = 5$.

Reduced triangular basis over $p = 5$. The OM algorithm run with precision 69 finds a factorisation $f = f_1\,f_2\,f_3$, for which we have initial approximations

$$\psi_1 = x^4 + 2\,p^{24}, \psi_2 = \phi_1^2 + p^{18}\,\phi_1 + p^{32}\,x + p^{36}, \psi_3 = \phi_1 + p^{17}$$

with $\phi_1 = x^3 + p^8\,x + p^{12}$. It provides the three associated quasi-valuations w_1, w_2, w_3 satisfying (we denote $\overrightarrow{w}\,(a) = (w_1(a), w_2(a), w_3(a))$):

$$\overrightarrow{w}\,(x) = (6,4,4)\ ;\ \overrightarrow{w}\,(\phi_1) = (12,18,17)$$
$$\overrightarrow{w}\,(f_1) = (\infty,16,16)\ ;\ \overrightarrow{w}\,(f_2) = (24,\infty,34)\ ;\ \overrightarrow{w}\,(f_3) = (12,17,\infty)$$

We also get $w_1(\psi_1) = 24$, $w_2(\psi_2) = 36$, $w_3(\psi_3) = 17$ and the numerator sets are

$$\mathcal{N}_{5,1} = \{1, x, x^2, x^3, f_1\}; \mathcal{N}_{5,2} = \{1, x, x^2, \phi_1, x\,\phi_1, x^2\,\phi_1, f_2\}; \mathcal{N}_{5,3} = \{1, x, x^2, f_3\}.$$

`MaxMin` runs as follows: starting from $g_0 = 1$, at each step i, we increase in the triplet the index equal to the smallest $j \in \{1,2,3\}$ s.t. $w_j(g_i) = \min w(g_i)$ (which is underlined in the last column).

i	triplet	g_i	$\overrightarrow{w}\,(g_i)$	$w(g_i)$
0	$(0,0,0)$	1	$(\underline{0},0,0)$	0
1	$(1,0,0)$	x	$(6,\underline{4},4)$	4
2	$(1,1,0)$	x^2	$(12,\underline{8},8)$	8
3	$(1,2,0)$	x^3	$(18,\underline{12},12)$	12
4	$(1,3,0)$	$x\,\phi_1$	$(\underline{18},22,21)$	18
5	$(2,3,0)$	$x^2\,\phi_1$	$(\underline{24},26,25)$	24
6	$(3,3,0)$	$x^3\,\phi_1$	$(30,30,\underline{29})$	29
7	$(3,3,1)$	$x^4\,\phi_1$	$(36,34,\underline{33})$	33
8	$(3,3,2)$	$x^5\,\phi_1$	$(42,38,\underline{37})$	37
9	$(3,3,3)$	$x^3\,\phi_1\,f_3$	$(\underline{42},47,\infty)$	42
10	$(4,3,3)$	$\phi_1\,f_1\,f_3$	$(\infty,\underline{51},\infty)$	51
11	$(4,4,3)$	$x\,\phi_1\,f_1\,f_3$	$(\infty,\underline{55},\infty)$	55
12	$(4,5,3)$	$x^2\,\phi_1\,f_1\,f_3$	$(\infty,\underline{59},\infty)$	59

Note that any order on the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ works here. We get:

$$\mathcal{N}_5 = \{1, x, x^2, x^3, x\,\phi_1, x^2\,\phi_1, x^3\,\phi_1, x^4\,\phi_1, x^5\,\phi_1, x^3\,\phi_1\,f_3, \phi_1\,f_1\,f_3, x\,\phi_1\,f_1\,f_3, x^2\,\phi_1\,f_1\,f_3\}$$

Finally, one can check that it is sufficient to get approximations ψ_i of the factors f_i satisfying $w_1(\psi_1) \geq 28$, $w_2(\psi_2) \geq 36$ (that we got from the OM algorithm with precision 69) and $w_3(\psi_3) \geq 18$. By lifting the factorisation only once (using precision 70), we get that, and update:

$$\psi_1 = x^4 + 2\,p^{24} + p^{34}\ ,\ \psi_3 = \phi_1 + p^{17} + 2\,p^{12}\,x^2 + 4\,p^{16}\,x + 3\,p^{20}$$

Reduced triangular basis over $p = 2$. Here we do not need the `MaxMin` algorithm. As $f \mod 2 = (y^3+y^2+1)\,(y^4+y^3+1)\,(y^3+y+1)^2$, we only use the OM algorithm above the factor $(y^3 + y + 1)$, then use Proposition 6 to conclude. The OM algorithm provides a local set of numerators equal to $\{1, x, x^2, \phi_0, x\,\phi_0, x^2\,\phi_0\}$ with $\phi_0 = x^3 + x + 1$. We thus get

$$\mathcal{N}_2 = \{1, x, x^2, x^3, x^4, x^5, x^6, g, x\,g, x^2\,g, \phi_0\,g, x\,\phi_0\,g, x^2\,\phi_0\,g\}$$

with $g = (x^3 + x^2 + 1)\,(x^4 + x^3 + 1)$.

Global basis. We finally glue together these two bases using CRT. For instance, we compute g_4 s.t. $g_4 = x^4 + 5^8\,x^2 + 5^{12}\,x \mod 5^{19}$ and $g_4 = x^4 \mod 2$, that is $g_4 = 5^{19}\,x^4 - 2^{\frac{5^{19}-1}{2}}(x^4 + 5^8\,x^2 + 5^{12}\,x) = x^4 + (5^8 - 5^{27})\,x^2 + (5^{12} - 5^{31})\,x$, using $5^{19} - 2^{\frac{5^{19}-1}{2}} = 1$. We get similar formulas for g_5 and g_6 (replacing 19 by resp. 25 and 30), etc. Computing all the g_i this way, we get the following global triangular integral basis:

$$\{1, \frac{\theta}{5^4}, \frac{\theta^2}{5^8}, \frac{\theta^3}{5^{12}}, \frac{g_4(\theta)}{5^{18}}, \frac{g_5(\theta)}{5^{24}}, \frac{g_6(\theta)}{5^{29}}, \frac{g_7(\theta)}{5^{33}}, \frac{g_8(\theta)}{5^{37}}, \frac{g_9(\theta)}{5^{42}}, \frac{g_{10}(\theta)}{2\,5^{51}}, \frac{g_{11}(\theta)}{2\,5^{55}}, \frac{g_{12}(\theta)}{2\,5^{59}}\}$$

In particular, we get $D_f = 2^3\,5^{372}$ mentioned earlier.

References

1. Abelard, S.: On the complexity of computing integral bases of function fields. In: Proceedings of Computer Algebra in Scientific Computing (CASC). pp. 42–62. CASC 2020, Springer International Publishing (2020)
2. Bauch, J.D.: Lattices over polynomial Rings and Applications to Function Fields. Ph.D. thesis, Universitat Autònoma de Barcelona (2014)
3. Bauch, J.D.: Computation of integral bases. Journal of Number Theory **165**, 382–407 (2016). https://doi.org/https://doi.org/10.1016/j.jnt.2016.01.011, https://www.sciencedirect.com/science/article/pii/S0022314X16000743
4. Bauch, J.D., Nart, E., Stainsby, H.: Complexity of the OM factorizations of polynomials over local fields. LMS Journal of Computation and Mathematics **16**, 139–171 (2013)
5. Böhm, J., Decker, W., Laplagne, S., Pfister, G.: Computing integral bases via localization and hensel lifting. Journal of Symbolic Computation **109**, 283–324 (2022). https://doi.org/https://doi.org/10.1016/j.jsc.2020.07.007, https://www.sciencedirect.com/science/article/pii/S0747717120300626
6. Bürgisser, P., Clausen, M., Shokrollahi, A.: Algebraic Complexity Theory, vol. 315 (01 1997). https://doi.org/10.1007/978-3-662-03338-8
7. Cohen, H.: Advanced Topics in Computational Number Theory. Graduate texts in mathematics, Springer New-York, NY (2012)
8. Ford, D., Pauli, S., Roblot, X.F.: A fast algorithm for polynomial factorization over qp. Journal de Théorie des Nombres de Bordeaux **14**, 151–169 (2002)
9. Gathen, J.v.z., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, New York, NY, USA, 3rd edn. (2013)
10. Guàrdia, J., Montes, J., Nart, E.: Newton polygons of higher order in algebraic number theory. Transactions of the American Mathematical Society **364**, 361–416 (2012)
11. Guàrdia, J., Montes, J., Nart, E.: A new computational approach to ideal theory in number fields. Foundations of Computational Mathematics **13**, 729–762 (2013)
12. Guàrdia, J., Montes, J., Nart, E.: Higher newton polygons and integral bases. Journal of Number Theory **147**, 549–589 (2015). https://doi.org/https://doi.org/10.1016/j.jnt.2014.07.027, https://www.sciencedirect.com/science/article/pii/S0022314X14002777
13. Hallouin, E.: Computing local integral closures. Journal of Symbolic Computation **32**(3), 211–230 (2001)

14. Hess, F.: Computing Riemann–Roch spaces in algebraic function fields and related topics. Journal of Symbolic Computation **33**(4), 425–445 (2002). https://doi.org/https://doi.org/10.1006/jsco.2001.0513, https://www.sciencedirect.com/science/article/pii/S0747717101905139
15. van Hoeij, M.: An algorithm for computing an integral basis in an algebraic function field. Journal of Symbolic Computation **18**, 353–363 (1994)
16. Hoeven, J.v.d., Lecerf, G.: Directed evaluation. Journal of Complexity **60**, 101498 (2020)
17. Mac Lane, S.: A construction for prime ideals as absolute values of an algebraic field. Duke Math. J. **2**(3), 492–510 (1936), https://doi.org/10.1215/S0012-7094-36-00243-0
18. MacLane, S.: A construction for absolute values in polynomial rings. Trans. Amer. Math. Soc. **40**(3), 363–395 (1936), https://doi.org/10.2307/1989629
19. Nart, E.: Local computation of differents and discriminants. Mathematics of Computation **83**(287), 1513–1534 (2014)
20. Okutsu, K.: Construction of integral basis, I. Proc. Japan Acad. Ser. A Math. Sci. **58**(1), 47–49 (1982). https://doi.org/10.3792/pjaa.58.47, https://doi.org/10.3792/pjaa.58.47
21. Okutsu, K.: Construction of integral basis, I. Proc. Japan Acad. Ser. A Math. Sci. **58**(4), 167–169 (1982)
22. Peral, J.M.: Polígonos de newton de orden superior y aplicaciones aritméticas. Ph.D. thesis, Universitat de Barcelona (1999)
23. Pohst, M.: Computational Algebraic Number Theory. Birkhauser Verlag (1993)
24. Poteaux, A., Weimann, M.: Local polynomial factorisation: Improving the montes algorithm. In: Proceedings of the 2022 ACM on International Symposium on Symbolic and Algebraic Computation. pp. 149–158. ISSAC '22, ACM, New York, NY, USA (2022)
25. Stainsby, H.D.: Triangular bases of integral closures. Journal of Symbolic Computation **87**, 140–175 (2018)
26. Stainsby, H.D.: Triangular bases of integral closures. Ph.D. thesis, Universitat Autònoma de Barcelona (2014)
27. Villard, G.: Elimination ideal and bivariate resultant over finite fields. In: Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation. pp. 526–534. ISSAC '23, Association for Computing Machinery, New York, NY, USA (2023)